Zeitschrift für Datenrecht und Informationssicherheit

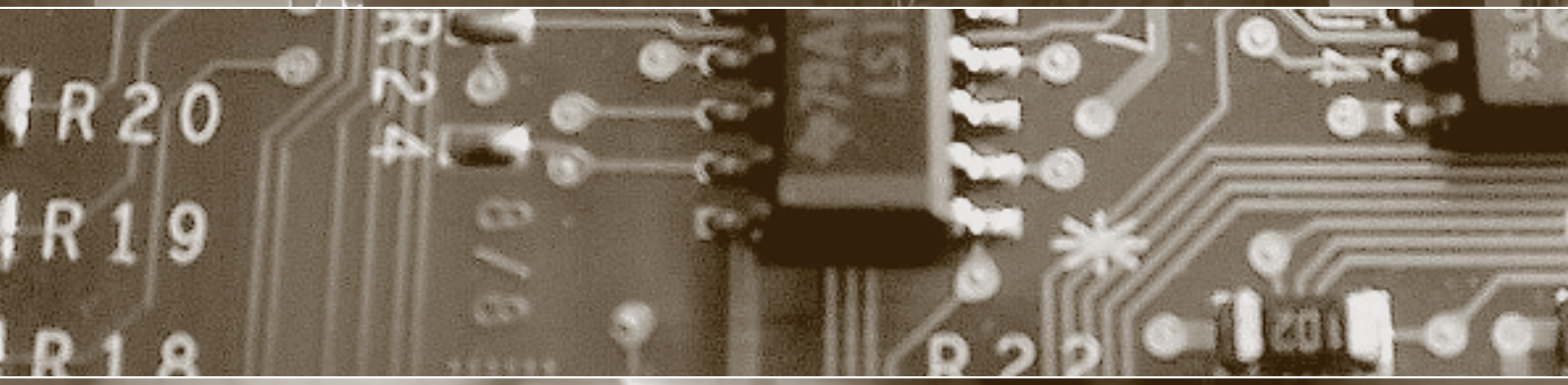
digma

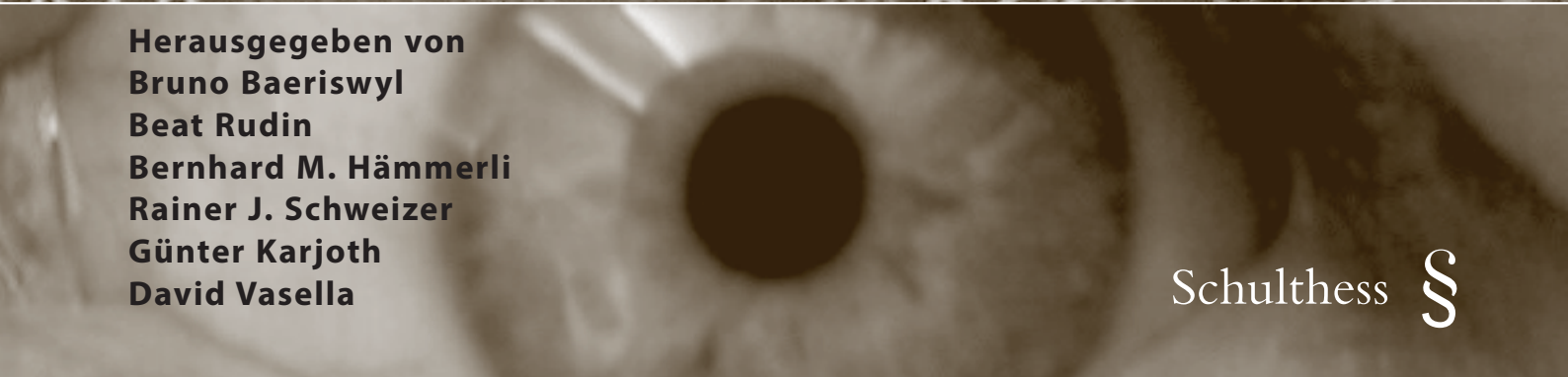
www.digma.info 18. Jahrgang, Heft 3, September 2018

Schwerpunkt:

Cybersouveränität

fokus: Digitale Selbstbestimmung der Schweiz
fokus: Unterschätzte Risiken durch Lieferanten
report: RGPD en Suisse: mise en œuvre des sanctions





Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth
David Vasella

Schulthess §

inhalt

fokus

Schwerpunkt:
Cybersouveränität

Digitale Selbstbestimmung der Schweiz

Der Begriff «Cybersouveränität» ist international von Staaten besetzt, die das Internet auf nationaler Ebne kontrollieren wollen. Es sollte daher besser von «digitaler Selbstbestimmung» gesprochen werden. Wie setzt sich die Schweiz auf internationaler Ebene dafür ein?

Cybersouveränität aus völkerrechtlicher Warte

Wird durch Cyberoperationen die völkerrechtliche Souveränität eines Staates verletzt, hat dieser zwar ein Recht auf Selbstverteidigung und zur Ergreifung von Gegenmassnahmen. Aufgrund faktischer Hürden – namentlich fehlender eigener Cyberfähigkeiten zur Entdeckung und Zuordnung eines Angriffs und Ausführung eines digitalen Gegenschlags – greifen diese völkerrechtlichen Mittel der Selbsthilfe allerdings oft ins Leere. Politisch anzusetzen ist deshalb bei der Prävention gegen schädliche Cyberoperationen.

Sicherheitspolitik und digitale Souveränität

Angesichts der neuen Sicherheitsherausforderungen im Zuge der Digitalisierung braucht es dringend nachhaltige Konzepte und Strategien, um die öffentliche Sicherheit, die Sicherheitsvorsorge und vor allem Transparenz für die Bürgerinnen und Bürger und damit deren Vertrauen sicherzustellen.

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Prof. Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. (em.) Dr. iur. Rainer J. Schweizer, Prof. Dr. Günter Karjoth, Dr. iur. David Vasella

Redaktion: Dr. iur. Bruno Baeriswyl und Prof. Dr. iur. Beat Rudin

Rubrikenredaktor(inn)en: Dr. iur. Barbara Widmer, Dr. iur. Dominika Blonski

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Inland: CHF 174.00, Jahresabo Ausland: CHF 199.00, Einzelheft: CHF 48.00
PrintPlu§: Jahresabo Inland: CHF 195.00, Jahresabo Ausland CHF 220.00

PrintPlu§: Das PrintPlu§-Abonnement bietet die Möglichkeit, bequem und zeitgleich zur Printausgabe jeweils das PDF der ganzen Ausgabe herunterzuladen. Detaillierte Informationen finden Sie unter www.schulthess.com/printplus.

Anzeigenverkauf und -beratung: Fachmedien Zürichsee Werbe AG, Laubisrütistrasse 44, CH-8712 Stäfa,
Tel. +41 (0)44 928 56 11, pietro.stuck@fachmedien.ch

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach 2218, CH-8021 Zürich
Tel. +41 (0)44 200 29 29, Fax +41 (0)44 200 29 28, service@schulthess.com, www.schulthess.com

Unterschätzte Risiken durch Lieferanten

Mit der zunehmenden digitalen Vernetzung der Unternehmen im Cyber-Raum werden Anreize und Angriffsflächen für Attacken grösser. Unternehmen haben daher den Schutz ihrer eigenen Infrastruktur in den letzten Jahren stark verbessert. Doch wie kann sich ein Unternehmen gegen Angriffe auf seine Lieferanten schützen?

RGPD sur sol suisse: mise en œuvre

Die EU-Datenschutz-Grundverordnung kann auf Schweizer Unternehmen Anwendung finden. Wie werden allfällige von EU-Datenschutzbehörden ausgesprochene Sanktionen durchgesetzt werden?

Was klar scheint, muss nicht klar sein

Die EU-Datenschutz-Grundverordnung gilt auch, wenn Unternehmen in Drittstaaten Personen, die sich in der EU befinden, Dienstleistungen anbieten und in diesem Zusammenhang Personendaten über diese Personen bearbeiten. Alles klar?

Cybersouveränität

In einer zunehmend vernetzten Welt wird es auch zunehmend schwierig, die Souveränität sicherzustellen. Systemkomponenten müssen sorgfältig evaluiert werden. Unser Cartoonist war dabei …

Cybersouveränität aus völkerrechtlicher Warte

Das Interventions- und das Gewaltverbot gelten auch im Cyberspace

Anna Petrig, Prof. Dr., Professorin für Völkerrecht und Öffentliches Recht, Universität Basel anna.petrig@unibas.ch

Maria Stemmler, Ass. iur. und M.A. Philosophie, wissenschaftliche Assistentin, Universität Basel, Doktorandin an der Albert-Ludwigs-Universität Freiburg, Deutschland maria.stemmler@unibas.ch

Cyberspionage, internetgestützte politische Einflussnahme und digitale Angriffe auf kritische Infrastrukturen können die völkerrechtliche Souveränität verletzen.

Die zunehmende Verbreitung von Cybertechnologien führt zu einer neuen Verwundbarkeit der Staaten. Berichte über Cyberoperationen, mit denen Wahlen beeinflusst, Infrastrukturen lahmgelegt oder Cyberspionage ermöglicht werden soll – wie jüngst beim bundesnahen Technologiekonzern RUAG Holding AG[1] – gehören mittlerweile zur medialen Tagesordnung. Dies wirft die Frage auf, ob und unter welchen Voraussetzungen solche Vorgänge einen Eingriff in die völkerrechtliche Souveränität des betroffenen Staates darstellen, namentlich gegen das Interventions- und das Gewaltverbot verstossen.

Die Analyse wird zeigen, dass diese beiden elementaren Verbote grundsätzlich auch im Cyberspace greifen. Allerdings müssen sie spezifisch für den virtuellen Raum übersetzt werden. Ein prominentes Beispiel einer solchen Transposition allgemein gehaltener und vor einem anderen Hintergrund entstandener Völkerrechtsregeln auf den Cyberkontext stellt das *Tallinn Manual*[2] dar, in dem eine Gruppe von Experten zentrale Völkerrechtsregeln auf Cyberoperationen angewandt und heruntergebrochen hat. Vorliegend wird ähnlich verfahren und skizzenhaft dargestellt, wie das Konzept der Souveränität – das mit Fug und Recht als Dreh- und Angelpunkt des Völkerrechts bezeichnet werden kann – im Lichte des Cyberraums gelesen werden kann.

Was bedeutet völkerrechtliche Souveränität?

Das Konzept der Souveränität nimmt eine zentrale Stellung im völkerrechtlichen Gefüge ein. Aus ihm lassen sich die meisten anderen Prinzipien und Institute direkt oder zumindest indirekt ableiten. Obwohl – oder gerade weil – es sich bei der Souveränität um eine Schlüsselfigur des Völkerrechts handelt, ist es kein leichtes Unterfangen, sie definitorisch klar zu umreissen. Üblicherweise werden zwei Seiten des Prinzips voneinander abgegrenzt: die Souveränität «nach innen» und die Souveränität «nach aussen»[3].

Mit «innerer» Souveränität ist gemeint, dass der Staat nach innen die höchste und einzige Gewalt innehat, die auch als staatliche Hoheitsgewalt bezeichnet wird. Sie beinhaltet namentlich die Gebiets- und Personalhoheit: Der Staat darf Regeln bezüglich Menschen, Dingen und Vorgängen in seinem Territorium erlassen, für seine Staatsangehörigen auch ausserhalb. Er kann die von ihm gesetzten Regeln durchsetzen (z.B. durch die Polizei) und über Rechtsfragen entscheiden (z.B. durch seine Zivil- und Strafgerichte)[4]. In Bezug auf den Cyberspace bedeutet dies u.a., dass ihm die Entscheidung obliegt, ob und inwiefern die auf seinem Territorium befindliche Cyberinfrastruktur an das Internet angeschlossen wird bzw. bleibt. Er verfügt zudem über vielfältige Möglichkeiten zur Regulierung von Teilen des Cyberspace. Zu betonen ist, dass sich aus der Hoheitsgewalt nicht nur Rechte, sondern auch Pflichten ergeben. In Bezug auf den Cyberspace ist namentlich die *due diligence*-Pflicht interessant, auf die zurückzukommen sein wird.

Zunächst interessiert uns aber die sogenannte «äussere» Souveränität. Sie besagt, dass die Staaten nur dem Völkerrecht, nicht aber einem anderen Staat unterstellt sind; Souveränität in diesem Sinne ist also (rechtliche) Unabhängigkeit von anderen Staaten. Daraus fliessen zwei weitere für das Völkerrecht zentrale Grundsätze, nämlich das Verbot der Einmischung in innere und äussere Angelegenheiten eines anderen Staates (sogenanntes Interventionsverbot) und das Verbot, gegen einen anderen Staat Gewalt anzudrohen oder anzuwenden (sogenanntes Gewaltverbot)[5].

Interventions- und Gewaltverbot

Vereinfacht gefasst verwehrt das Interventionsverbot den Staaten, sich unter Anwendung

oder Androhung von Zwang in die inneren und äusseren Angelegenheiten anderer Staaten einzumischen. Es schützt somit das Recht eines jeden Staates, sein politisches, soziales, wirtschaftliches und kulturelles System frei zu wählen und seine Aussenbeziehungen frei zu gestalten. Ein Staat soll diesbezüglich Entscheidungsfreiheit geniessen und sein Wille nicht durch Zwang den Interessen eines fremden Staates unterworfen werden[6].

Die Schwierigkeit liegt darin, eine verbotene Intervention von einer erlaubten Einwirkung auf die innen- oder aussenpolitischen Aktivitäten eines anderen Staates abzugrenzen, die in einer interdependenten Staatengemeinschaft durchaus erwünscht ist. Das Abgrenzungskriterium liegt im sogenannten Zwangselement. Erst wenn Zwang vorliegt, wird in der Regel eine Einmischung im Völkerrecht als verbotene Intervention qualifiziert. Das fragliche Vorgehen muss daher das Potenzial haben, den betroffenen Staat zu einem Verhalten zu bewegen, das er andernfalls nicht an den Tag gelegt hätte. Der Begriff deckt sich allerdings nicht generell mit jenem der Alltagssprache[7]. Ob einer Massnahme Zwang innewohnt, wird auch gestützt auf weitere Kriterien ermittelt: dem tatsächlichen Erfolg, der Mittel-Zweck-Relation sowie der Intensität der Massnahme[8]. Um im Cyberbereich zwischen zulässiger Einmischung und verbotener Intervention zu unterscheiden, wird vielfach auf die Intensität der Massnahme abgestellt.

Droht ein Staat gegenüber einem anderen mit Gewalt oder wendet er solche an, liegt nicht nur eine verbotene Intervention, sondern auch ein Verstoss gegen das Gewaltverbot vor. Unter den Gewaltbegriff fallen nicht nur die klassische militärische Gewaltanwendung, sondern – und dies ist für den Cyberspace von Bedeutung – auch Handlungen, die vergleichbaren physischen Zwang beinhalten[9]. Auch hier ist wiederum die Intensität der Handlung ausschlaggebend: Sie muss eine Mindestschwelle an physischer Zwangswirkung überschreiten. Bislang scheint noch kein (bekannt gewordener) Cyberangriff die Schwelle des Gewaltverbots klar überschritten zu haben.

Wer kann die Souveränität eines Staates verletzen?

Da das Souveränitätsprinzip das Verhältnis der Staaten untereinander regelt, kann die Souveränität eines Staates grundsätzlich auch nur von anderen Staaten verletzt werden – nicht aber durch Private. Privatpersonen, namentlich transnationale Wirtschaftskonzerne, sind zwar faktisch durchaus in der Lage, die staatliche Handlungsfreiheit erheblich zu beeinträchtigen oder gar Schäden innerhalb und ausserhalb des Cyberspace zu verursachen. Dadurch greifen sie allerdings nicht in die völkerrechtliche Souveränität des betroffenen Staates ein; begehen aber unter Umständen eine Straftat im Zusammenhang mit dem Cyberspace. Diese sogenannten *cybercrimes* werden unter anderem im Übereinkommen über die Cyberkriminalität des Europarats vom 23. November 2001 definiert, das von der Schweiz ratifiziert wurde[10].

Aus der äusseren Souveränität fliessen zwei für das Völkerrecht zentrale Grundsätze, nämlich das Interventionsverbot und das Gewaltverbot.

Eine Ausnahme vom Grundsatz, dass das Handeln Privater keinen Eingriff in die Souveränität eines Staates darstellen kann, besteht allerdings, sofern ihr Tun einem Staat zugerechnet werden kann. Dies ist in unterschiedlichen Konstellationen möglich, so wenn es in seinem Auftrag oder unter seiner Leitung bzw. Kontrolle stattfindet oder er es als sein eigenes anerkennt und annimmt[11].

Souveränitätsverletzungen durch Cyberoperationen

Aber wann liegt eine Verletzung der Cybersouveränität eines Staates, konkret eine Verletzung des Interventions- und Gewaltverbots, vor? Zur Beantwortung dieser Frage muss der Begriff des Cyberspace kurz definiert werden. Mitunter wird er synonym mit dem des Internets verwendet. Tatsächlich werden ihm aber auch weitere Strukturen zugerechnet, wie Telekommunikationsnetze oder Computersysteme. Daher lässt sich der Cyberspace als virtueller Raum be-

Kurz&bündig

Die zunehmende Verbreitung von Cybertechnologien führt zu einer neuen Verwundbarkeit der Staaten. Cyberoperationen zwecks Wahlbeeinflussung, Lahmlegung von Infrastrukturen oder Spionage zeugen davon. Solche Operationen können die völkerrechtliche Souveränität des Zielstaates verletzen, namentlich gegen das Interventions- oder Gewaltverbot verstossen. Staaten, die Ziel eines solchen Cyberangriffs sind, haben zwar ein Recht auf Selbstverteidigung bzw. ein Recht zur Ergreifung von Gegenmassnahmen. Aufgrund faktischer Hürden – namentlich fehlender eigener Cyberfähigkeiten zur Entdeckung und Zuordnung eines Angriffs und Ausführung eines digitalen Gegenschlags – greifen diese völkerrechtlichen Mittel der Selbsthilfe allerdings oft ins Leere. Politisch anzusetzen ist deshalb bei der Prävention gegen schädliche Cyberoperationen.

zeichnen, in dem mittels digitaler Technologien und Vernetzung Daten erzeugt, abgelegt, verändert und ausgetauscht werden[12]. Dem Cyberraum werden unterschiedliche Ebenen zugeordnet: eine physische, die aus den physischen Netzwerkkomponenten besteht; eine logische, die die Verbindungen zwischen den Netzwerkgeräten umfasst; und schliesslich eine soziale, auf der Individuen und Gruppen agieren[13]. Handlungen, welche die Möglichkeiten des Cyberspace nutzen, um Ziele im Cyberraum oder vermittels seiner zu erreichen, können als Cyberoperationen bezeichnet werden[14].

Ab wann überschreiten Versuche der Wahlbeeinflussung per Cyberoperation die Schwelle des Interventionsverbotes und sind folglich als Souveränitätsverletzung zu werten?

Als weltweiter Raum entzieht sich der Cyberspace einer eindeutigen geografischen und damit auch territorialen Verortung. Sowohl involvierte Personen als auch technische Anlagen sind über den Globus verteilt. Aufgrund dessen untersteht der Cyberraum *als Ganzes* nicht der Hoheitsgewalt eines *einzelnen* Staates. Es wäre aber dennoch falsch, zu behaupten, dass er sich der völkerrechtlichen Souveränität vollständig entzieht. Tatsächlich manifestiert sich staatliche Souveränität auf allen drei Ebenen des Cyberspace. Ein grosser Teil der Cyberinfrastruktur befindet sich auf dem Territorium von Staaten und untersteht somit ihrer Hoheitsgewalt. Ebenso werden die Verbindungen zwischen den Netzwerken innerhalb ihres Territoriums erfasst. Nicht zuletzt unterstehen Personen, die von ihrem Territorium aus Cyberoperationen vornehmen, ihrer Souveränität[15].

Diese Cybersouveränität kann in der Folge auch durch andere Staaten verletzt werden. Drei in ihrer Zielrichtung unterschiedliche Formen von Cyberoperationen – politische Einflussnahme, die Beeinträchtigung kritischer Infrastrukturen und Spionage – werden nun auf die Frage hin untersucht, ob sie eine Souveränitätsverletzung darstellen. Konkret, ob sie gegen das Interventions- oder das Gewaltverbot verstossen.

Politische Einflussnahme via Cyberspace

Versuchte Wahlbeeinflussung per Cyberoperation ist derzeit in aller Munde. Aber ab wann überschreiten derartige Aktivitäten die Schwelle des Interventionsverbotes und sind folglich als Souveränitätsverletzung zu werten? Wie erwähnt, ist hierfür eine unzulässige Einmischung in die inneren oder äusseren Angelegenheiten eines Staates durch einen anderen Staat erforderlich.

Eine hinreichend qualifizierte Verletzung wird angenommen, wenn ein anderer Staat in einen staatlichen Wahlvorgang eingreift, beispielsweise durch die Verfälschung elektronisch generierter Abstimmungsergebnisse[16]. Hinsichtlich der rein inhaltlichen Beeinflussung von Wahlkämpfen ist der gegenwärtige Stand ein anderer. Sofern lediglich polemische oder kritische Äusserungen getätigt werden, kommt ein Verstoss gegen das Interventionsverbot nicht in Betracht. Die Grenze ist allerdings überschritten, sobald die Beiträge der Aufwiegelung dienen oder Hetzpropaganda darstellen[17].

Die Beurteilung jüngerer Vorfälle hängt somit von den konkreten Umständen und Inhalten ab. Die Veröffentlichung vertraulicher Dokumente aus den Wahlkampagnen Hillary Clintons und Emmanuel Macrons, die durch *hacks* erlangt wurden[18], ist danach wohl nicht als Souveränitätsverletzung zu werten. Die Einstufung der Schaltung von Werbung und der Verwendung von *fake accounts* in sozialen Netzwerken, wie sie im US-Wahlkampf 2016 beobachtet wurden[19], muss danach anhand der tatsächlich publizierten Botschaften vorgenommen werden. Eine Souveränitätsverletzung ist möglich, aber nicht zwingend.

Cyberoperationen gegen kritische Infrastrukturen

Auch Cyberoperationen, die auf Teile der Infrastruktur eines Staates gerichtet sind, können eine Souveränitätsverletzung darstellen. Das Augenmerk liegt dabei auf Vorfällen, von denen *kritische* Infrastrukturen betroffen sind; also solche, deren Funktionieren für ein staatliches Gemeinwesen essenziell ist, wie Kraftwerke als Teile der Energieversorgung oder Krankenhäuser als Zentren medizinischer Versorgung. Dazu zählen auch Strukturen der Telekommunikation und der Informationstechnologie.

Das Vorliegen einer Souveränitätsverletzung ist auch hier anhand der bekannten Kriterien zu beurteilen, wobei die Intensität der Einwirkung von besonderem Gewicht ist. Danach bleiben Aktivitäten, mittels derer in ein wichtiges Netzwerk des Staates (wie in jenes des Deutschen Bundestages 201 5[20]) eingedrungen und Dokumente ausgespäht werden, regelmässig unterhalb der Schwelle des Interventionsverbotes[21]. Etwas anderes wird vertreten, wenn Websites staatlicher Stellen und des privaten

Sektors über mehrere Wochen hinweg von aussen blockiert werden, um den betroffenen Staat zu einer anderen Politik zu drängen – wie dies wohl 2007 in Estland der Fall war[22]. Insbesondere in Anbetracht der Relevanz von Computersystemen für die Erfüllung öffentlicher Aufgaben können derartige Eingriffe als verbotene Intervention eingestuft werden[23]. Bewirken Cyberoperationen einen dauerhaften Funktionalitätsverlust der fraglichen Infrastruktur, so ist regelmässig von einer verbotenen Intervention auszugehen. Als Beispiel hierfür kann die Beschädigung tausender Festplatten des staatlichen Erdölförderunternehmens *Saudi Aramco* 2012 angeführt werden, sofern sie von einer anderen staatlichen Seite ausging[24].

Haben Cyberoperationen erhebliche Sach- oder gar Personenschäden zur Folge, ist schliesslich die Grenze zum Gewaltverbot überschritten. In diese Kategorie könnte die Beschädigung iranischer Urananreicherungszentrifugen durch den Computerwurm *Stuxnet* fallen[25]. Andere, bislang theoretische und deutlich gravierendere Beispiele für eine Verletzung des Gewaltverbotes durch Cyberoperationen wären der manipulationsbedingte Ausfall der Flugsicherung eines Staates, der in Flugzeugabstürzen resultiert, oder die Herbeiführung eines nuklearen Störfalls[26].

Cyberspionage: jenseits völkerrechtlicher Souveränität?

Die völkerrechtliche Zulässigkeit von Spionage bleibt umstritten. Einigkeit besteht weitgehend dahin, dass Spionage zwischen Staaten an sich – mit wenigen Ausnahmen – nicht generell verboten ist. Sofern sie auf die Ausspähung von Privatpersonen gerichtet ist, kann sie aber Menschenrechte (z.B. das Recht auf Achtung des Privatlebens) und damit auch wiederum das Völkerrecht verletzen[27]. Dessen ungeachtet steht es den Staaten frei, Spionage in ihrem nationalen Recht unter Strafe zu stellen und zu verfolgen. Dieser Rahmen gilt grundsätzlich auch für Cyberspionage, bei der nicht öffentlich verfügbare Daten des Staates oder seiner Wirtschaft heimlich bzw. unter Vorspiegelung falscher Tatsachen mittels Cyberoperation abgeschöpft werden[28].

Bislang ungeklärt ist, ob Cyberspionage, die von *ausserhalb* des Zielstaates erfolgt, ab einer gewissen Schwere eine Souveränitätsverletzung darstellt. Während einige darin einen Verstoss gegen das Interventionsverbot sehen, lehnen dies andere unter Verweis auf den mangelnden Zwangscharakter der Massnahme ab[29]. Nach der ersten Ansicht könnte die bereits erwähnte Ausspähung des Netzwerkes des Deutschen Bundestages eine Verletzung des Interventionsverbotes darstellen, sofern sie eine gewisse Schwere erreicht hat. Das Gleiche gälte für das aus der Ferne erfolgte Abhören von Diensthandys von Spitzenpolitikern – also für Vorfälle, wie sie im Zuge der Snowden-Enthüllungen 2013 bekannt wurden[30]. Wird die Cyberoperation durch eine Tätigkeit *auf dem Territorium* des betroffenen Staates ermöglicht, beispielsweise durch das Einstecken eines USB-Sticks in einen Computer im Zielstaat oder durch das Anzapfen eines Unterwasserkabels in den Territorialgewässern eines Staates, kommt eine Souveränitätsverletzung in Betracht. Werden durch Cyberspionage oder durch ihre Ermöglichung physische oder sonst vergleichbare Schäden verursacht – ungeachtet, von wo aus die Spionage erfolgt –, steht wiederum ein Verstoss gegen das Interventions- oder gar das Gewaltverbot im Raum.

Das Anlegen sogenannter *honeypots,* also scheinbar wertvoller Datenbestände oder Netzwerksegmente, mit denen ein Staat Informationen über den abschöpfenden Akteur sammelt, wird grundsätzlich als zulässige Souveränitätsausübung betrachtet. Zielen die bereitgestellten Datensätze allerdings darauf ab, Störungen oder Schäden im Zielsystem zu bewirken, dann wird dies teilweise als Völkerrechtsverstoss gewertet. Andere Stimmen kommen zu dem Schluss, dass die fraglichen Schäden durch den abschöpfenden Staat selbst in sein System verbracht wurden und daher keine Zurechnung zum Errichter der Falle infrage kommt[31].

Aktivitäten, mittels derer in ein wichtiges Netzwerk des Staates eingedrungen und Dokumente ausgespäht werden, bleiben regelmässig unterhalb der Schwelle des Interventionsverbotes.

Reaktionsmöglichkeiten des betroffenen Staates

Was aber kann ein Staat, dessen Souveränität durch eine Cyberoperation verletzt wurde, tun? Darf er mit eigenen computergestützten Angriffen oder gar mit militärischer Gewalt antworten? Das Völkerrecht sieht für Souveränitätsverletzungen vor allem zwei Reaktionsmöglichkeiten vor: Selbstverteidigung und Gegenmassnahmen. Diese Abwehrmöglichkeiten können theoretisch auch gegen Cyberangriffe eingesetzt werden – allerdings stehen ihrer Verwendung in der Praxis oft nahezu unüberwindbare praktische Hürden im Wege.

Zunächst muss eine die Souveränität eines Staates verletzende Cyberoperation entdeckt werden. Dass dies nicht trivial ist, belegt die eindrückliche Zahl von 150 bis 200 Tagen, die es in der deutschen Industrie durchschnittlich braucht, um eine Netzwerk-Penetration zu erkennen. Viele werden nie als solche erkannt, weil ein unmittelbarer Zusammenhang zwischen Einsatz und Wirkung fehlt; und viele sind gar darauf angelegt, unerkannt zu bleiben, wie beispielsweise Ausspähungen[32]. Wird ein Angriff entdeckt, liegt die nächste faktische Herausforderung darin, die Urheber der Cyberoperation zu identifizieren. Da der Netzwerkcharakter des Cyberspace effektive Möglichkeiten der Verschleierung bietet, ist dies nicht einfach. So lassen anspruchsvoll gestaltete Cyberoperationen nicht nur wenige Spuren zu ihrer Identität zurück, sie werden auch häufig unter Verwendung manipulierter Rechner ahnungsloser Dritter durchgeführt, die über den ganzen Erdball verstreut sein können. Die Ermittlung der Verantwortlichen ist daher in der Regel ein zeit- und ressourcenintensives Unterfangen[33]. Ist ein Angriff entdeckt und dessen Urheberschaft ausgemacht, ist alsdann zu prüfen, ob die rechtlichen Voraussetzungen zur Ausübung des Selbstverteidigungsrechts bzw. zur Ergreifung von Gegenmassnahmen erfüllt sind.

Das Völkerrecht sieht für Souveränitätsverletzungen vor allem zwei Reaktionsmöglichkeiten vor: Selbstverteidigung und Gegenmassnahmen.

Staaten haben dann ein Recht auf Selbstverteidigung, wenn ein sogenannter «bewaffneter Angriff» gegen sie im Gange ist bzw. unmittelbar bevorsteht. Nicht jede unter das Gewaltverbot fallende Anwendung von Gewalt stellt bereits einen bewaffneten Angriff dar. Als solche gelten nur koordinierte Militärschläge, deren Ausmass und Auswirkungen von erheblichem Gewicht sind. Die Mittel, von denen die Gewalt ausgeht, sind dabei grundsätzlich unerheblich, womit auch mittels Cyberoperationen bewaffnete Angriffe durchgeführt werden können – vorausgesetzt, diese sind hinsichtlich Ausmass und Auswirkungen mit einem konventionellen Angriff vergleichbar[34]. Dies ist regelmässig dann der Fall, wenn Cyberangriffe Todesopfer, Verletzte oder erhebliche Sachschäden zeitigen. Die teilweise vertretene Ansicht, dass auch Cyberoperationen, die kritische Infrastrukturen beeinträchtigen und *keine* physischen Schäden nach sich ziehen, als bewaffneter Angriff zu werten sind, konnte sich bislang als zu grosse Ausweitung des Selbstverteidigungsrechts nicht durchsetzen[35].

Steht dem angegriffenen Staat das Selbstverteidigungsrecht zu, ist er in dessen Ausübung aber nicht frei. Seine Reaktion muss vielmehr notwendig und verhältnismässig sein sowie unmittelbar erfolgen[36]. Auch hier dürfte es aufgrund der noch in den Kinderschuhen steckenden Cyberforensik und der beschränkten Cyberfähigkeiten vieler angegriffener Staaten schwierig sein, alle drei kumulativen Anforderungen an die Selbstverteidigungshandlung zu erfüllen. Sofern eine Cyberoperation erst mit erheblicher Verzögerung entdeckt wird, ist das zeitliche Erfordernis der unmittelbaren Verteidigungshandlung auch bei schneller Reaktion nach Erkennen häufig nicht mehr einzuhalten. Betroffenen Staaten wird zwar durchaus zugestanden, Ursache und Urheber gründlich zu ermitteln. Bis sie handeln, darf aber nicht zu viel Zeit vergehen[37]. Soll die Abwehrhandlung zudem im Cyberspace erfolgen, ist es nicht einfach, das Verhältnismässigkeitsprinzip zu wahren: Gezielte und in ihren Wirkungen voraussehbare digitale Gegenschläge durchzuführen, ist äusserst anspruchsvoll, da sie u.a. detaillierte Kenntnis des Zielsystems und seiner Schwachstellen erfordern[38]. Insgesamt scheint die rechtmässige Ausübung des Selbstverteidigungsrechts – trotz allen Drängens auf Ermöglichung sogenannter *hack back operations*[39] – bei Cyberangriffen somit regelmässig an tatsächlichen Gründen zu scheitern.

Dasselbe gilt auch für sogenannte Gegenmassnahmen, die Staaten, die Opfer eines Völkerrechtsbruchs geworden sind, zwecks Selbsthilfe ergreifen dürfen. Dabei handelt es sich um gewaltfreie Akte, die für sich genommen gegen das Völkerrecht verstossen, aber aufgrund des vorangehenden Völkerrechtsbruchs gerechtfertigt sind. Auch die Ausübung dieses Rechts ist an eine Reihe von Voraussetzungen geknüpft: Gegenmassnahmen dürfen von einem betroffenen Staat nur ergriffen werden, wenn sie darauf abzielen, eine noch andauernde Völkerrechtsverletzung zu unterbinden, und gegen deren Urheber gerichtet sind. Sie müssen zudem verhältnismässig sein und angekündigt werden[40].

Staaten, die Gegenmassnahmen gegen völkerrechtsverletzende Cyberoperationen einleiten wollen, stehen vor ähnlichen Schwierigkeiten wie diejenigen, die von ihrem Recht auf Selbstverteidigung Gebrauch machen wollen. Ein Unterschied besteht allerdings hinsichtlich des Zeitfaktors: Gegenmassnahmen dürfen auch ergriffen werden, wenn ein anderer Staat für bereits beendete Völkerrechtsverletzungen

keine Wiedergutmachung leistet[41]. Da dies bei erst spät aufgedeckten Cyberoperationen regelmässig der Fall sein dürfte, stünde dem betroffenen Staat in dieser Konstellation unter Umständen das Recht zu, Gegenmassnahmen zu ergreifen.

Insgesamt lässt sich feststellen, dass Cyberoperationen durchaus das Interventions- und gar das Gewaltverbot – und somit die staatliche Souveränität – verletzen können. Obwohl das Völkerrecht die Abwehr solcher Angriffe mittels Selbstverteidigung oder Gegenmassnahmen vorsieht, können deren Voraussetzungen aufgrund der beschränkten Cyberfähigkeiten der angegriffenen Staaten oftmals nicht erfüllt werden und greifen somit ins Leere. Daher ist es zentral, dass alle Staaten auf die Unterbindung und Beendigung von schädlichen Cyberoperationen hin- und zusammenarbeiten. Dies ist nicht nur ein politisches Desiderat, sondern ergibt sich (jedenfalls zum Teil) aus der völkerrechtlichen *due diligence*-Pflicht der Staaten, die sich ebenfalls aus der Souveränität ableitet.

Die Voraussetzungen von Selbstverteidigung oder Gegenmassnahmen können aufgrund der beschränkten Cyberfähigkeiten der angegriffenen Staaten oftmals nicht erfüllt werden.

Fussnoten

1 Surber Michael, Cyberangriff auf Ruag – Lob und Tadel für das Verteidigungsdepartement, NZZ Online, 8.5.2018, <www.nzz.ch>.
2 Schmitt Michael (Hrsg.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge 2017.
3 Besson Samantha, Sovereignty (April 2011), in: Wolfrum Rüdiger (Hrsg.), Max Planck Encyclopedia of Public International Law, <http://www.opil.ouplaw.com>, Rn. 1 ff., 69.
4 Peters Anne, Völkerrecht, 4. Aufl., 2016, 33, Rn. 20.
5 Peters (Fn. 4), 33, Rn. 20 f.
6 Vgl. dazu insges. von Arnauld Andreas, Völkerrecht, 3. Aufl., 2016, 151, Rn. 349 f.
7 Arnauld (Fn. 6), 153 f., Rn. 359.
8 Peters (Fn. 4), 318, Rn. 49.
9 Vgl. insges. Arnauld (Fn. 6), 459 f., Rn. 1031 f.
10 SR 311.43.
11 Vgl. dazu Artikel der Völkerrechtskommission zur Verantwortlichkeit der Staaten für völkerrechtswidrige Handlungen, UN-GV Res. 56/83 vom 12.12.2001.
12 Vgl. dazu Schaller Christian, Internationale Sicherheit und Völkerrecht im Cyberspace, SWP-Studie 2014/S 18, Oktober 2014, 5.
13 Tallinn Manual (Fn. 2), 12, Nr. 4.
14 US DOD Dictionary of Military and Associated Terms, Stand Juni 2018, Eintrag *cyberspace operations,* <http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf>.
15 Vgl. Tallinn Manual (Fn. 2), 11, Nr. 1 und 14, Nr. 4–7; vgl. zudem Schaar Peter, Digitale Souveränität, digma 2015, 40 f.
16 Vgl. Schaller (Fn. 12), zudem Tallinn Manual (Fn. 2), 22, Nr. 16.
17 Vgl. insges. Arnauld (Fn. 6), Rn. 364, zudem auch Tallinn Manual (Fn. 2) 26, Nr. 29.
18 Harding Luke, Top Democrat's emails hacked by Russia after aide made typo, investigation finds, The Guardian, 14.12.2016, <http://www.theguardian.com>; Denkler Thorsten, Emmanuel Macron beklagt Hacker-Angriff, Süddeutsche Zeitung, 6.5.2017, <http://www.sueddeutsche.de>.
19 Solon Olivia/Siddiqui Sabrina, Russia-backed Facebook posts ‹reached 126m Americans› during US election, The Guardian, 31.10.2017, <http://www.theguardian.com>.
20 Baumgärtner Maik/Röbel Sven/Wiedmann-Schmidt Wolf, Hacker kopierten Abgeordneten-E-Mails, Spiegel Online, 18.6.2015, <http://www.spiegel.de>.
21 Vgl. Tallinn Manual (Fn. 2) 323, Nr. 33.
22 Buchan Russell, Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?, 17 Journal of Conflict & Security Law (2012) 211, 218 f., zudem 225 f.
23 Arnauld (Fn. 6), Rn. 360, Schaller (Fn. 12), 17.
24 Vgl. insges. Tallinn Manual (Fn. 2), 20 f.
25 Vgl. insges. Schaller (Fn. 12), 17.
26 Buchan (Fn. 22), 212.
27 Schaller (Fn. 12), 11 ff.
28 Schaller (Fn. 12), 11.
29 Vgl. insges. Tallinn Manual (Fn. 2), 170 f., Nr. 8.
30 Vgl. Arnauld (Fn. 6), 156 f., Rn. 369.
31 Vgl. insges. Tallinn Manual (Fn. 2), 171, Nr. 10 f.
32 Vgl. dazu insges. Schulze Matthias, Hacking back? Technische und politische Implikationen digitaler Gegenschläge, SWP-Aktuell 2017/A 59, August 2017, 1 f.
33 Vgl. dazu insges. Schulze (Fn. 32), 2, und Schaller (Fn. 12), 21.
34 Vgl. insges. Arnauld (Fn. 6), 480 f., Rn. 1077 f.
35 Vgl. insges. Schaller (Fn. 12), 18 f.; s. auch Tallinn Manual (Fn. 2), 342 f., Nr. 10, 12.
36 Tallinn Manual (Fn. 2), 348 ff.
37 Schaller (Fn. 12), 22.
38 Schulze (Fn. 32), 2.
39 Vgl. dazu und zu *hack backs* generell: Reinhold Thomas/Schulze Matthias, Digitale Gegenangriffe, SWP-Arbeitspapier, August 2017, 1 ff.
40 Vgl. insges. Arnauld (Fn. 6), 178 ff., 419 ff.
41 Arnauld (Fn. 6), 178, 419.
42 Vgl. insges. Arnauld (Fn. 6), 146, Rn. 340; 347, Rn. 793.
43 Tallinn Manual (Fn. 2), 30, Regel 6.
44 Tallinn Manual (Fn. 2), 40, Nr. 37.
45 Vgl. insges. Tallinn Manual (Fn. 2), 43, Regel 7 und Nr. 1.
46 Schaller (Fn. 12), 23.
47 Tallinn Manual (Fn. 2), 31 f., Nr. 5; 45, Nr. 8.
48 Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022, April 2018, <http://www.newsd.admin.ch/newsd/message/attachments/52071.pdf>, 2.
(Alle URL letztmals kontrolliert am. 19.8.2018.)

Souveränität beinhaltet auch Pflichten – *due diligence*

Das völkerrechtliche Konzept der Souveränität beinhaltet nicht nur Rechte, sondern auch Pflichten für Staaten. Wir haben gesehen, dass aus der «inneren» Souveränität die staatliche Hoheitsgewalt fliesst, welche namentlich Gebiets- und Personalhoheit umfasst. Daraus ergibt sich die Pflicht eines jeden Staates, gemäss der gebotenen Sorgfalt *(due diligence)* dafür zu sorgen, dass von seinem Territorium aus keine schädigenden Handlungen gegenüber anderen Staaten vorgenommen werden[42].

Verschiedene Staaten haben deshalb Cyberstrategien verabschiedet, welche der eigenen digitalen Verwundbarkeit entgegenwirken sollen.

Wie erwähnt, erstreckt sich die staatliche Souveränität auch auf den Cyberraum, und Staaten üben Hoheitsgewalt auf allen drei Ebenen des Cyberspace aus: Während die physische und die logische Ebene ihrer Gebietshoheit unterfallen, wird die soziale Ebene von der Personalhoheit erfasst. Es herrscht daher im Grundsatz Einigkeit darüber, dass die *due diligence*-Pflicht auch im Cyberraum greift. Entsprechend wird im *Tallinn Manual* die Regel formuliert, dass ein Staat die gebotene Sorgfalt walten lassen muss, damit sein Territorium oder seiner faktischen Kontrolle unterstehende Cyberinfrastruktur (wie Server und Netze im Ausland, auf die er Zugriff hat) nicht für Cyberoperationen genutzt werden, welche in die (souveränen) Rechte anderer Staaten eingreifen und ernsthafte nachteilige Folgen für diese zeitigen[43].

Hat ein Staat, beispielsweise aufgrund geheimdienstlicher Informationen, Kenntnis davon[44], dass von Personen oder Infrastruktur, die unter seiner Hoheitsgewalt stehen, derartige Cyberoperationen ausgehen, ist er zum Einschreiten verpflichtet. Gemäss *Tallinn Manual* muss er alle in der gegebenen Situation durchführbaren Massnahmen treffen, um die Schädigungshandlung zu beenden. Diese Wortwahl spiegelt wider, dass wenig Einigkeit darin besteht, welche konkreten Schritte der Gefahrenabwehr ein Staat zu unternehmen hat[45]. Zu den möglichen Massnahmen zählt, dass ein (ungewollt) an einer Cyberoperation beteiligter Staat den Zielstaat vor der Cyberoperation warnt bzw. darüber informiert und sich an ihrer Abwehr und Aufklärung beteiligt[46].

Der Dissens ist noch grösser bei der Frage, ob die völkerrechtliche *due diligence*-Pflicht Staaten sogar verpflichtet, *präventiv* tätig zu werden, um schädigende Cyberoperationen zu verhindern. Dass die völkerrechtliche Sorgfaltspflicht im Bereich des Cyberspace neben einem repressiven auch ein präventives Element beinhaltet, wird weitgehend abgelehnt[47]. Auch wenn grundsätzlich keine völkerrechtliche Pflicht zur Verhütung schädlicher Cyberoperationen besteht, tun Staaten gut daran, sich in diesem Bereich zu engagieren. Denn ist ein Cyberangriff einmal im Gange, ist dessen (rechtmässige) Abwehr nicht einfach durchzuführen. Verschiedene Staaten haben deshalb Cyberstrategien verabschiedet, welche der eigenen digitalen Verwundbarkeit entgegenwirken sollen. So jüngst auch die Schweiz, deren zweite Cyberstrategie für die Jahre 2018–2022 «den strategischen Rahmen für die Verbesserung der Prävention, Früherkennung, Reaktion und Resilienz in allen in Bezug auf Cyber-Risiken relevanten Bereichen» bildet[48]. ■